Pacific Journal of Mathematics

ON A THEOREM OF HEGYVÁRI AND HENNECART

DAO NGUYEN VAN ANH, LE QUANG HAM,
DOOWON KOH, THANG PHAM AND LE ANH VINH

Volume 305 No. 2 April 2020

PACIFIC JOURNAL OF MATHEMATICS
Vol. 305, No. 2, 2020
dx.doi.org/10.2140/pjm.2020.305.407

ON A THEOREM OF HEGYVÁRI AND HENNECART

DAO NGUYEN VAN ANH, LE QUANG HAM,
DOOWON KOH, THANG PHAM AND LE ANH VINH

We study growth rate of product of sets in the Heisenberg group over finite fields and the complex numbers. More precisely, we will give improvements and extensions of recent results due to Hegyvári and Hennecart (2018).

1. Introduction

Let $\mathbb{F}_q$ be an arbitrary finite field with order $q = p^r$ for some positive integer r and an odd prime p. For an integer $n \geq 1$, the Heisenberg group of degree n, denoted by $H_n(\mathbb{F}_q)$, is defined by a set of the following matrices:

$$[\boldsymbol{x}, \boldsymbol{y}, z] := \begin{bmatrix} 1 & \boldsymbol{x} & z \\ \mathbb{0} & I_n & \boldsymbol{y}^t \\ 0 & \mathbb{0} & 1 \end{bmatrix}$$

where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, $z \in \mathbb{F}_q$, $\boldsymbol{y}^t$ denotes the column vector of $\boldsymbol{y}$, and I_n is the $n \times n$ identity matrix. For $A \subset \mathbb{F}_q$, $E, F \subset \mathbb{F}_q^n$, we define

$$[E, F, A] := \{[\boldsymbol{x}, \boldsymbol{y}, z] : \boldsymbol{x} \in E, \boldsymbol{y} \in F, \ z \in A\},$$

and

$$[E, F, A][E, F, A] := \{[\boldsymbol{x}, \boldsymbol{y}, z] \cdot [\boldsymbol{x}', \boldsymbol{y}', z'] : [\boldsymbol{x}, \boldsymbol{y}, z], [\boldsymbol{x}', \boldsymbol{y}', z'] \in [E, F, A]\},$$

Over recent years, there is an intensive study on growth rate in the Heisenberg group over finite fields and applications. Hegyvári and Hennecart [2013] proved a structure result for *bricks* in Heisenberg groups. The precise statement is as follows.

Theorem 1.1 [Hegyvári and Hennecart 2013]. *For every $\epsilon > 0$, there exists a positive integer $n_0(\epsilon)$ such that for all $n \geq n_0(\epsilon)$ and any sets $X_i, Y_i, Z \subset \mathbb{F}_p$, $i \in [n]$, $X = \prod_{i=1}^n X_i \subset \mathbb{F}_p^n$, $Y = \prod_{i=1}^n Y_i \subset \mathbb{F}_p^n$, if*

$$(1) \qquad |[X, Y, Z]| > |H_n(\mathbb{F}_p)|^{3/4+\epsilon},$$

then $[X, Y, Z][X, Y, Z]$ contains at least $|[X, Y, Z]|/p$ cosets of $[\mathbb{0}, \mathbb{0}, \mathbb{F}_p]$.

MSC2010: 11T06, 11T55, 20G40.
Keywords: finite fields, matrix, sum-product estimates, incidences.

It follows from the proof of Theorem 1.1 in [Hegyvári and Hennecart 2013] that $\epsilon = O(1/n)$. In a very recent work, Shkredov [2020] obtained the following theorem which improves the relation between ϵ and n in the specific case when sizes of sets X_i, Y_i, Z are comparable.

Theorem 1.2 [Shkredov 2020]. *Let $n \geq 2$ be an even number, and $X_i, Y_i, Z \subset \mathbb{F}_p$, $i \in [n]$, $X = \prod_{i=1}^n X_i \subset \mathbb{F}_p^n$, $Y = \prod_{i=1}^n Y_i \subset \mathbb{F}_p^n$ such that X_i, Y_i have comparable sizes. Set $\mathcal{X} = \max_i |X_i|$ and $\mathcal{Y} = \max_i |Y_i|$. If $|Z| \leq \mathcal{X}\mathcal{Y}$, $\mathcal{X} \leq |Z|\mathcal{Y}$, $\mathcal{Y} \leq |Z|\mathcal{X}$ and*

$$\mathcal{X}\mathcal{Y} \gtrsim p^{3/2} \cdot \left(\frac{\mathcal{X}\mathcal{Y}}{p|Z|^{1/2}}\right)^{2^{-n/2}}, \tag{2}$$

then $[X, Y, Z][X, Y, Z]$ contains at least $|[X, Y, Z]|/p$ cosets of $[\mathbb{0}, \mathbb{0}, \mathbb{F}_p]$.

Suppose that $X_i = Y_j = Z$ for all $1 \leq i, j \leq n$. Then it follows from Theorem 1.2 that $[X, Y, Z][X, Y, Z]$ contains at least $|[X, Y, Z]|/p$ cosets of $[\mathbb{0}, \mathbb{0}, \mathbb{F}_p]$ under the condition $|Z| \gtrsim p^{3/4+1/(2^{n/2+4}-12)}$, which improves the threshold $p^{3/4+O(1/n)}$ of Theorem 1.1. Moreover, Shkredov [2020] gives an introduction to representation theory which is good for products of general sets in the affine and in the Heisenberg groups.

Throughout this paper, we use $X \ll Y$ if $X \leq CY$ for some constant $C > 0$ independent of the parameters related to X and Y, and write $X \gg Y$ for $Y \ll X$. The notation $X \sim Y$ means that both $X \ll Y$ and $Y \ll X$ hold. In addition, we use $X \lesssim Y$ to indicate that $X \ll (\log_2 Y)^{C'} Y$ for some constant $C' > 0$.

It is worth noting that there is an interesting application of products of sets in the Heisenberg group to so-called models of *Freiman isomorphisms*; see [Hegyvári and Hennecart 2012]. Moreover, it has been indicated in [Tao and Vu 2006, §5.3] that any set in the Heisenberg group with the doubling constant less than two does not have any good model.

It is well-known that there is a connection between the sum-product phenomenon and growth in the group of affine transformations, for example, see [Rudnev and Shkredov 2018]. Such a connection has been discovered in the setting of Heisenberg group by Hegyvári and Hennecart [2018]. More precisely, in the case $n = 1$, using sum-product estimates, they proved that if $A \subset \mathbb{F}_p$ with $|A| \geq p^{1/2}$, then

$$|[A, A, 0][A, A, 0]| \gg \min\{p^{1/2}|[A, A, 0]|^{5/4},\ p^{-1/2}|[A, A, 0]|^2\}. \tag{3}$$

When the size of A is not too big, the authors obtained the following.

Theorem 1.3 [Hegyvári and Hennecart 2018]. *Let A be a set in $\mathbb{F}_p$. Suppose that $|A| \leq p^{2/3}$, then we have*

$$|[A, A, 0][A, A, 0]| \gg |[A, A, 0]|^{7/4}.$$

Notice that the method in the proof of Theorem 1.3 can be extended to arbitrary finite fields, and as a consequence, we obtain the following.

Theorem 1.4 [Hegyvári and Hennecart 2018]. *Let A be a set in $\mathbb{F}_q$. Suppose that $|A| \geq q^{2/3}$, then we have*

$$|[A, A, 0][A, A, 0]| \gg q|[A, A, 0]|.$$

Note that the lower bound in Theorem 1.4 is stronger than that of (3).

The main purpose of this paper is to give improvements and extensions of Theorems 1.3 and 1.4 in the setting of arbitrary finite fields $\mathbb{F}_q$ and the complex numbers $\mathbb{C}$.

In our first theorem, we will show that Theorem 1.4 can be improved in the case where the additive energy of A is small.

Theorem 1.5. *Let A be a set in $\mathbb{F}_q$. Let $\Lambda^+(A)$ be the number of quadruples $(a, b, c, d) \in A^4$ such that $a + b = c + d$. Suppose that $\Lambda^+(A) \leq |A|^3/K$ for some $K > 0$ and $|A| \geq K^{1/3}q^{2/3}$, then we have*

$$|[A, A, 0][A, A, 0]| \gg Kq|[A, A, 0]|.$$

Our next theorem is an extension of Theorem 1.4 in the setting of $H_n(\mathbb{F}_q)$ for any $n \geq 1$.

Theorem 1.6. *Let E be a set in $\mathbb{F}_q^n$. Suppose that $|E| \gg q^{n/2+1/4}$, then we have*

$$|[E, E, 0][E, E, 0]| \gg q|[E, E, 0]|.$$

Notice that in general the conclusion of Theorem 1.6 is sharp, since E can be a subspace in $\mathbb{F}_q^n$, which implies that $[E, E, 0][E, E, 0] \subset [E, E, \mathbb{F}_q]$. Moreover, the exponent $\frac{1}{2}n + \frac{1}{4}$ can not be decreased to $\frac{1}{2}n$, since, supposing that $q = p^2$, one can take $E = \mathbb{F}_p^n$, which gives us $|[E, E, 0][E, E, 0]| \ll p|[E, E, 0]| = q^{1/2}|[E, E, 0]|$.

In the setting of prime fields, if E is a set in the plane $\mathbb{F}_p^2$ and the size of E is not too big, then we have the following theorem in $H_2(\mathbb{F}_p)$.

Theorem 1.7. *Let $\mathbb{F}_p$ be a prime field with $p \equiv 3 \bmod 4$, and E be a set in $\mathbb{F}_p^2$ with $|E| \ll p^{8/5}$. Then*

$$|[E, E, 0][E, E, 0]| \gg |[E, E, 0]|^{19/15}.$$

When A is a multiplicative subgroup of $\mathbb{F}_p^*$, we are able to show that the exponent $\frac{7}{4}$ in Theorem 1.3 can be improved significantly.

Theorem 1.8. *Let A be a multiplicative subgroup of $\mathbb{F}_p^*$ with $|A| \leq p^{1/2} \log p$. We have*

$$|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{151/80}.$$

In the setting of the real numbers, for any $A \subset \mathbb{R}$, using a point-plane incidence bound due to Elekes and Tóth [2005] and an energy variant of the sum-product conjecture due to Rudnev, Shkredov, and Stevens [Rudnev et al. 2020], Hegyvári and Hennecart [2018] proved that

$$|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{15/8}.$$

In our next theorem, we employ a point-line incidence bound over the complex numbers due to Tóth [2015] and an energy variant of the sum-product conjecture due to Rudnev, Shkredov, and Stevens [Rudnev et al. 2020] to study an extension in the setting of the complex numbers.

Theorem 1.9. *Let A be a set in $\mathbb{C}$ with $|A| \geq 2$. We have*

$$|[A, A, 0][A, A, 0]| \gtrsim |A|^{29/8} = |[A, A, 0]|^{29/16}.$$

2. Proof of Theorem 1.5

To prove Theorem 1.5, we need to recall a lemma given by the third, fourth, and fifth listed authors in [Koh et al. 2018].

Let X be a multiset in $\mathbb{F}_q^{2n} \times \mathbb{F}_q$. We denote by $\overline{X}$ the set of distinct elements in the multiset X. The cardinality of X, denoted by $|X|$, is $\sum_{x \in \overline{X}} m_X(x)$, where $m_X(x)$ is the multiplicity of $\boldsymbol{x}$ in X. For multisets $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q^{2n+1}$, let $N(\mathcal{A}, \mathcal{B})$ be the number of pairs $((\boldsymbol{a}, b), (\boldsymbol{c}, d)) \in \mathcal{A} \times \mathcal{B} \subset (\mathbb{F}_q^{2n} \times \mathbb{F}_q)^2$ such that $\boldsymbol{a} \cdot \boldsymbol{c} = b + d$. We have the following lemma on an upper bound of $N(\mathcal{A}, \mathcal{B})$.

Lemma 2.1 [Koh et al. 2018, Lemma 8.1]. *Let $\mathcal{A}, \mathcal{B}$ be multisets in $\mathbb{F}_q^{2n} \times \mathbb{F}_q$. We have*

$$\left| N(\mathcal{A}, \mathcal{B}) - \frac{|\mathcal{A}||\mathcal{B}|}{q} \right| \leq q^n \left(\sum_{(a,b) \in \overline{\mathcal{A}}} m_{\mathcal{A}}((a, b))^2 \sum_{(c,d) \in \overline{\mathcal{B}}} m_{\mathcal{B}}((c, d))^2 \right)^{1/2}.$$

Theorem 1.5 is a direct consequence of the following theorem.

Theorem 2.2. *For $A \subset \mathbb{F}_q$, we have*

$$|[A, A, 0][A, A, 0]| \gg \min\left\{ \frac{|A|^5}{q}, \frac{q|A|^5}{\Lambda^+(A)} \right\}.$$

Proof. Without loss of generality, we assume that $0 \notin A$. Let S be the number of quadruples of matrices (m_1, m_2, m_3, m_4) in $[A, A, 0]^4$ such that $m_1 m_2 = m_3 m_4$. By the Cauchy–Schwarz inequality, we have

$$|[A, A, 0]^2| \geq \frac{|A|^8}{S}.$$

To complete the proof, it will be enough to show that

$$S \ll \frac{|A|^3\Lambda^+(A)}{q} + q|A|^3.$$

In the next step we are going to prove this. Indeed, from the definition of S, we have that S is equal to the number of tuples $(a, b, c, d, a', b', c', d')$ in A^8 such that

$$a + c = a' + c', \tag{4}$$

$$b + d = b' + d', \tag{5}$$

$$ad = a'd'. \tag{6}$$

It follows from (4) and (5) that $a = a' + c' - c$ and $d' = b + d - b'$. Substituting into (6), we obtain

$$(a' + c' - c) \cdot d = a' \cdot (b + d - b').$$

This implies that

$$d(c' - c) = a'(b - b'). \tag{7}$$

In case $b \neq b'$, we also have $c \neq c'$, since $0 \notin A$. In this case, the above equality is equivalent with

$$a' = \frac{d}{b - b'}(c' - c).$$

It follows from (7) that if $b = b'$ then $c = c'$. We note that the number of tuples $(a', b, b', c, c', d) \in A^6$ with $b = b'$ and $c = c'$ is at most $|A|^4$. We now count the number of tuples with $b \neq b'$ and $c \neq c'$. It follows from (4), (5), and (6) that the number of tuples $(a, b, c, d, a', b', c', d') \in A^8$ satisfying these equalities is at most the number of tuples $(a', c, c', b, b', d) \in A^6$ such that

$$a' = \frac{d}{b - b'}(c' - c) \quad \text{and} \quad b + d - b' \in A.$$

Let X be the number of such tuples.

Define $P = A \times A$. Let L be the multiset of lines of the form $y = d/(b-b')(x-c)$ with $b + d - b' \in A$. It is clear that $|P| = |A|^2$ and $|L| = \Lambda^+(A)|A|$. One can check that X is bounded by the number of incidences between points in P and lines in L.

Let $\mathcal{L}$ be the multiset in $\mathbb{F}_q^2$ containing points of the form $(d/(b-b'), d/(b-b')\cdot c)$ with $b + d - b' \in A$ and $c \in A$. On the other hand, by an elementary calculation, we have $\sum_{l \in \bar{\mathcal{L}}} m_{\mathcal{L}}(l)^2 \leq X|A|$, and $|\mathcal{L}| = |L|$. With this new set $\mathcal{L}$, we have $X = N(P, \mathcal{L})$, where $N(P, \mathcal{L})$ is defined as in Lemma 2.1. Applying Lemma 2.1, we have

$$X \leq \frac{|A|^3\Lambda^+(A)}{q} + q^{1/2}X^{1/2}|A|^{3/2},$$

which implies that

$$X \leq \frac{|A|^3 \Lambda^+(A)}{q} + q|A|^3.$$

In other words, we have

$$S \leq \frac{|A|^3 \Lambda^+(A)}{q} + q|A|^3 + |A|^4 \ll \frac{|A|^3 \Lambda^+(A)}{q} + q|A|^3. \qquad \square$$

3. Proof of Theorem 1.6

In order to prove Theorem 1.6, we first prove the following lemma.

Lemma 3.1. *Let E be a set in $\mathbb{F}_q^n$. Let T be the number of triples $(\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{x}') \in E^3$ such that $\boldsymbol{v} \cdot (\boldsymbol{x} - \boldsymbol{x}') = 0$. Then we have*

$$T \leq \frac{|E|^3}{q} + q^n |E|.$$

Before proving Lemma 3.1, we need to review the Fourier transform of functions on $\mathbb{F}_q^n$. Let χ be a nontrivial additive character on $\mathbb{F}_q$. For a function $f : \mathbb{F}_q^n \to \mathbb{C}$, the Fourier transform of f, denoted by $\hat{f}$, is defined by

$$\hat{f}(\boldsymbol{m}) = q^{-n} \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} \chi(-\boldsymbol{x} \cdot \boldsymbol{m}) f(\boldsymbol{x}).$$

The following Fourier inversion theorem can be easily proved by the orthogonality relation of χ:

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{m} \in \mathbb{F}_q^n} \chi(\boldsymbol{x} \cdot \boldsymbol{m}) \hat{f}(\boldsymbol{m}).$$

It follows that

$$\sum_{\boldsymbol{m} \in \mathbb{F}_q^n} |\hat{f}(\boldsymbol{m})|^2 = q^{-n} \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} |f(\boldsymbol{x})|^2,$$

which is referred to as the Plancherel theorem.

We are now ready to prove Lemma 3.1.

Proof of Lemma 3.1. The number T can be expressed as follows:

$$\begin{aligned} T &= \sum_{\boldsymbol{x} \cdot \boldsymbol{v} - \boldsymbol{x}' \cdot \boldsymbol{v} = 0} E(\boldsymbol{v}) E(\boldsymbol{x}) E(\boldsymbol{x}') \\ &= \frac{|E|^3}{q} + \frac{1}{q} \sum_{s \neq 0} \sum_{\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_q^n} \chi(s\boldsymbol{v} \cdot (\boldsymbol{x} - \boldsymbol{x}')) E(\boldsymbol{v}) E(\boldsymbol{x}) E(\boldsymbol{x}') \\ &= \frac{|E|^3}{q} + q^{2n-1} \sum_{s \neq 0} \sum_{\boldsymbol{v} \in \mathbb{F}_q^n} |\widehat{E}(s\boldsymbol{v})|^2 E(\boldsymbol{v}). \end{aligned}$$

Using a change of variables by letting $\boldsymbol{z} = s\boldsymbol{v}$, we have

$$T \leq \frac{|E|^3}{q} + q^{2n} \sum_{\boldsymbol{z} \in \mathbb{F}_q^n} |\widehat{E}(\boldsymbol{z})|^2 = \frac{|E|^3}{q} + q^n |E|,$$

where we used $\sum_{\boldsymbol{z} \in \mathbb{F}_q^n} |\widehat{E}(\boldsymbol{z})|^2 = q^{-n}|E|$. □

We are ready to prove Theorem 1.6.

Proof of Theorem 1.6. Let $\boldsymbol{S}$ be the number of quadruples of matrices $(\boldsymbol{m}_1, \boldsymbol{m}_2, \boldsymbol{m}_3, \boldsymbol{m}_4)$ in $[E, E, 0]^4$ such that $\boldsymbol{m}_1\boldsymbol{m}_2 = \boldsymbol{m}_3\boldsymbol{m}_4$. By the Cauchy–Schwarz inequality, we have

$$|[E, E, 0][E, E, 0]| \geq \frac{|E|^8}{\boldsymbol{S}}.$$

In the next step, we are going to show that

$$\boldsymbol{S} \leq \frac{|E|^6}{q} + q^{n-1}|E|^4 + q^{2n}|E|^2.$$

Indeed, as in the proof of Theorem 2.2, we have that $\boldsymbol{S}$ is equal to the number of tuples $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{a}', \boldsymbol{b}', \boldsymbol{c}', \boldsymbol{d}')$ in E^8 such that

$$\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{a}' + \boldsymbol{c}', \tag{8}$$

$$\boldsymbol{b} + \boldsymbol{d} = \boldsymbol{b}' + \boldsymbol{d}', \tag{9}$$

$$\boldsymbol{a} \cdot \boldsymbol{d} = \boldsymbol{a}' \cdot \boldsymbol{d}'. \tag{10}$$

It follows from (8) and (9) that $\boldsymbol{a} = \boldsymbol{a}' + \boldsymbol{c}' - \boldsymbol{c}$ and $\boldsymbol{d}' = \boldsymbol{b} + \boldsymbol{d} - \boldsymbol{b}'$. Substituting into (10), we obtain

$$(\boldsymbol{a}' + \boldsymbol{c}' - \boldsymbol{c}) \cdot \boldsymbol{d} = \boldsymbol{a}' \cdot (\boldsymbol{b} + \boldsymbol{d} - \boldsymbol{b}').$$

This implies that

$$\boldsymbol{d} \cdot (\boldsymbol{c}' - \boldsymbol{c}) = \boldsymbol{a}' \cdot (\boldsymbol{b} - \boldsymbol{b}'). \tag{11}$$

For any tuples $(\boldsymbol{c}, \boldsymbol{c}', \boldsymbol{b}, \boldsymbol{b}', \boldsymbol{d}, \boldsymbol{a}')$ satisfying (11), we have $\boldsymbol{a}$ and $\boldsymbol{d}'$ are determined uniquely by (8) and (9).

Let $\mathcal{A}$ and $\mathcal{B}$ be multisets defined as follows:

$$\mathcal{A} = \{(\boldsymbol{d}, -\boldsymbol{b}, \boldsymbol{d} \cdot \boldsymbol{c}) : \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in E\}, \quad \mathcal{B} = \{(\boldsymbol{c}', \boldsymbol{a}', -\boldsymbol{a}' \cdot \boldsymbol{b}') : \boldsymbol{a}', \boldsymbol{b}', \boldsymbol{c}' \in E\}.$$

Let $N(\mathcal{A}, \mathcal{B})$ be the number defined as in Lemma 2.1. We have that the number of tuples satisfying (11) is equal to $N(\mathcal{A}, \mathcal{B})$.

To apply Lemma 2.1, we need to estimate $\sum_{\boldsymbol{x} \in \overline{\mathcal{A}}} m_{\mathcal{A}}(\boldsymbol{x})^2$ and $\sum_{\boldsymbol{y} \in \overline{\mathcal{B}}} m_{\mathcal{B}}(\boldsymbol{y})^2$.

We have

$$\sum_{\boldsymbol{x}\in\bar{\mathcal{A}}} m_{\mathcal{A}}(\boldsymbol{x})^2,\ \sum_{\boldsymbol{y}\in\bar{\mathcal{B}}} m_{\mathcal{B}}(\boldsymbol{y})^2 \le |E|T,$$

where T is the number of triples $(\boldsymbol{v}, \boldsymbol{x}, \boldsymbol{x}') \in E^3$ such that $\boldsymbol{v}\cdot(\boldsymbol{x}-\boldsymbol{x}')=0$.

On the other hand, Lemma 3.1 gives us

$$T \le \frac{|E|^3}{q} + q^n|E|.$$

Therefore, one can apply Lemma 2.1 with $|\mathcal{A}| = |\mathcal{B}| = |E|^3$ to derive

$$\boldsymbol{S} \le \frac{|E|^6}{q} + q^n\left(\frac{|E|^4}{q} + q^n|E|^2\right) \ll \frac{|E|^6}{q},$$

whenever $|E| \gg q^{(2n+1)/4}$. □

4. Proof of Theorem 1.7

To prove Theorem 1.7, we need to use the following lemmas. The first lemma is a consequence of the point-line incidence bound due to Stevens and de Zeeuw [2017]. To see a simple proof, see [Lund and Petridis 2018, Theorem 14].

Lemma 4.1. *Let P be a point set in $\mathbb{F}_p^2$ and L be a set of lines in $\mathbb{F}_p^2$. If $|P| \le p^{8/5}$, then the number of incidences between P and L, denoted by $I(P, L)$, satisfies*

$$I(P, L) \ll |P|^{11/15}|L|^{11/15} + |P| + |L|.$$

Lemma 4.2. *Let E be a set in $\mathbb{F}_p^2$ with $p \equiv 3 \mod 4$ and define $\Pi(E) := \{\boldsymbol{a}\cdot\boldsymbol{b} : \boldsymbol{a}, \boldsymbol{b} \in E\}$. If $|E| \le p^{8/5}$, then $|\Pi(E)| \gg |E|^{8/15}$.*

Proof. Since $p \equiv 3 \mod 4$, there is no isotropic line in $\mathbb{F}_p^2$. For each $\boldsymbol{a} \in E$, we denote the set $\{\boldsymbol{a}\cdot\boldsymbol{b} \colon \boldsymbol{b} \in E\}$ by $\Pi_{\boldsymbol{a}}(E)$. Suppose that

$$\max_{\boldsymbol{a}\in E} |\Pi_{\boldsymbol{a}}(E)| = t.$$

It is clear that $|\Pi(E)| \gg \max_{\boldsymbol{a}\in E} |\Pi_{\boldsymbol{a}}(E)|$.

Without loss of generality, we may assume that $0 \notin E$. We now fall into two following cases:

Case 1: If there is a line passing through the origin with at least m points of E, then those m points will contribute at least m distinct values to the set $\Pi(E)$. So, $|\Pi(E)| \gg m$.

Case 2: Suppose that all lines passing through the origin contain at most m points of E. This implies that the number of lines passing through the origin and a point in E is at least $|E|/m$.

Let L_0 be a set of lines passing through the origin and at least one point from E such that $|L_0| \sim |E|/m$. From each line l in L_0, we pick one point in $l \cap E$ arbitrarily, and let P be the set of those points. So $|P| = |L_0|$.

For any point $\boldsymbol{a} = (a_1, a_2) \in E$, let $L_{\boldsymbol{a}}$ be the set of lines defined by the equation $a_1 x + a_2 y = r$ with $r \in \Pi_{\boldsymbol{a}}(E)$. One can check that the size of $L_{\boldsymbol{a}}$ is the same as the size of $\Pi_{\boldsymbol{a}}(E)$. Moreover, we also have that $L_{\boldsymbol{a}} = L_{\boldsymbol{b}}$ when both a and b lie on a line in L_0, and $L_{\boldsymbol{a}} \cap L_{\boldsymbol{b}} = \varnothing$ when the $\boldsymbol{a}$ and $\boldsymbol{b}$ are distinct elements of P.

Let $L = \bigcup_{\boldsymbol{a} \in P} L_{\boldsymbol{a}}$. Since $|\Pi_{\boldsymbol{a}}(E)| \le t$ for any $\boldsymbol{a} \in E$, we have $|L_{\boldsymbol{a}}| \le t$ for all $\boldsymbol{a} \in E$. Thus $|L| \le |P| t = |L_0| t \sim |E| t/m$.

Let $I(E, L)$ be the number of incidences between E and L. For each $\boldsymbol{a} \in P$, we have $I(E, L_{\boldsymbol{a}}) = |E|$. Thus,

$$I(E, L) \gg |E|^2/m.$$

On the other hand, it follows from Lemma 4.1 that

$$I(E, L) \ll |E|^{11/15} (|E| t/m)^{11/15} + |E| + |E| t/m.$$

Hence, we have

$$|E|^2/m \ll |E|^{11/15} (|E| t/m)^{11/15} + |E| + |E| t/m.$$

Since $|E|^2/m \gg |E| + |E| t/m$, solving this inequality for t, we obtain $t \gg |E|^{8/11} m^{-4/11}$.

Optimizing two cases by choosing $m = |E|^{8/15}$, the lemma follows. □

Proof of Theorem 1.7. We first observe that

$$|[E, E, 0][E, E, 0]| \gg |\Pi(E)| |E|^2.$$

It follows from Lemma 4.2 that if $|E| \le p^{8/15}$ then we have

$$|\Pi(E)| \gg |E|^{8/15}.$$

Therefore,

$$|[E, E, 0][E, E, 0]| \gg |\Pi(E)| |E|^2 \gg |E|^{38/15},$$

whenever $|E| \ll p^{8/15}$. Since $|[E, E, 0]| = |E|^2$, this completes the proof. □

5. Proof of Theorem 1.8

In the proof of Theorem 1.8, the following results will be used.

Lemma 5.1. *Let A be a multiplicative subgroup of $\mathbb{F}_p^*$ with $|A| \lesssim p^{1/2}$. Let L be a set of lines in $\mathbb{F}_p^2$, and $I(A \times A, L)$ be the number of incidences between $A \times A$ and L. We have*

$$I(A \times A, L) \lesssim |A|^{4/3} |L|^{2/3}.$$

Proof. Let $T(A)$ be the number of collinear triples of points in $A \times A$. It has been shown in [Macourt et al. 2018, Theorem 1.2] that if $|A| \lesssim p^{1/2}$, then we have

$$T(A) \lesssim |A|^4.$$

For any $l \in L$, let $i(l)$ be the number of points of $A \times A$ on l. We have

$$I(A \times A, L) = \sum_{l \in L} i(l) \leq |L|^{2/3} \left(\sum_{l \in L} i(l)^3 \right)^{1/3} \ll |L|^{2/3} T(A)^{1/3} \lesssim |A|^{4/3} |L|^{2/3},$$

where we used the Hölder inequality in the inequality step. □

The following theorem is given in [Murphy et al. 2017, Theorem 3].

Theorem 5.2. *Let A be a multiplicative subgroup of $\mathbb{F}_p^*$. Suppose that $|A| \leq p^{1/2}$, then we have*

$$\Lambda^+(A) \lesssim |A|^{49/20}.$$

We are now ready to prove Theorem 1.8.

Proof of Theorem 1.8. We first repeat the first paragraph in the proof of Theorem 1.5.

Let S be the number of quadruples of matrices (m_1, m_2, m_3, m_4) in $[A, A, 0]^4$ such that $m_1 m_2 = m_3 m_4$. By the Cauchy–Schwarz inequality, we have

$$[|A, A, 0][A, A, 0]| \geq \frac{|A|^8}{S}.$$

Thus, to complete the proof, we only need to show that

$$S \lesssim |A|^4 + |A|^{169/40}.$$

Let X be the number of incidences between the point set $P = A \times A$ and the multiset L of lines of the form $y = d/(b - b')(x - c)$ with $b + d - b' \in A$. It is clear that $|P| = |A|^2$ and $|L| = \Lambda^+(A)|A|$. As in the proof of Theorem 2.2, we have $S \leq X + |A|^4$. Hence, it is enough to show that $|X| \lesssim |A|^{169/40}$.

For any line $l \in L$, let $m(l)$ be the multiplicity of l. By an elementary calculation,

$$\sum_{l \in \overline{L}} m(l)^2 \leq X|A|,$$

where $\overline{L}$ denotes the set of distinct lines in the multiset L. For $k \geq 1$, let L_k be the set of lines $l \in \overline{L}$ (without multiplicity) with $k \leq m(l) < 2k$. For any $k \geq 1$, we have

$$k|L_k| \leq |L| = \Lambda^+(A)|A|, \quad k^2 |L_k| \leq \sum_{l \in \overline{L}} m(l)^2 \leq X|A|.$$

Namely, we obtain

$$|L_k| \leq \min\left\{ \frac{\Lambda^+(A)|A|}{k}, \frac{X|A|}{k^2} \right\}, \tag{12}$$

for every $k \geq 1$.

For any line $l \in L$, let $i(l)$ be the size of $l \cap P$. Using Lemma 5.1 and (12), we have

$$
\begin{aligned}
I(P, L) & \\
&= \sum_{l \in \bar{L}} m(l) i(l) < \sum_i \sum_{l \in \bar{L},\, 2^i \leq m(l) < 2^{i+1}} 2^{i+1} \cdot i(l) \\
&= \sum_i 2^{i+1} \cdot I(P, L_{2^i}) \\
&= \sum_{i, 2^{i+1} \leq X/(\Lambda^+(A))} 2^{i+1} \cdot I(P, L_{2^i}) + \sum_{i,\, 2^{i+1} > X/(\Lambda^+(A))} 2^{i+1} \cdot I(P, L_{2^i}) \\
&\lesssim \sum_{i,\, 2^{i+1} \leq X/(\Lambda^+(A))} 2^{i+1} \cdot |A|^{4/3} \left(\frac{\Lambda^+(A)|A|}{2^i} \right)^{2/3} \\
&\qquad + \sum_{i,\, 2^{i+1} > X/(\Lambda^+(A))} 2^{i+1} \cdot |A|^{4/3} \left(\frac{X|A|}{2^{2i}} \right)^{2/3} \\
&\lesssim \sum_{i,\ 2^{i+1} \leq X/(\Lambda^+(A))} (2^i)^{1/3} |A|^2 \Lambda^+(A)^{2/3} + \sum_{i,\ 2^{i+1} > X/(\Lambda^+(A))} (2^i)^{-1/3} X^{2/3} |A|^2 \\
&\lesssim \sum_i \left(\frac{X}{\Lambda^+(A)} \right)^{1/3} |A|^2 \Lambda^+(A)^{2/3} + \sum_i \left(\frac{X}{\Lambda^+(A)} \right)^{-1/3} |A|^2 X^{2/3} \\
&\lesssim X^{1/3} |A|^2 \Lambda^+(A)^{1/3},
\end{aligned}
$$

where we have used the fact that each line in L has multiplicity at most $|A|^2$, which implies that $2^i \leq |A|^2$, so i is at most $2 \log_2 |A|$.

Since $X = I(P, L)$, we have proved that

$$X \lesssim |A|^2 X^{1/3} \Lambda^+(A)^{1/3},$$

which implies that $X \lesssim |A|^3 \Lambda^+(A)^{1/2}$. Applying Theorem 5.2, we have $X \lesssim |A|^{169/40}$, whenever $|A| \lesssim p^{1/2}$. This completes the proof of the theorem. □

6. Proof of Theorem 1.9

The proof of Theorem 1.9 is quite similar compared to that of Theorem 1.8. More precisely, we will need the following point-line incidence bound over the complex numbers due to Tóth [2015].

Theorem 6.1 [Tóth 2015]. *Let P be a set of points in $\mathbb{C}^2$ and L be a set of lines in $\mathbb{C}^2$. The number of incidences between P and L, denoted by $I(P, L)$, satisfies*

$$I(P, L) \ll |P|^{2/3} |L|^{2/3} + |P| + |L|.$$

Corollary 6.2 [Tóth 2015]. *Let P be a set of points in $\mathbb{C}^2$. For any integer $t \geq 2$, the number of lines containing at least t points from P is bounded by*

$$O\left(\frac{|P|^2}{t^3} + \frac{|P|}{t}\right).$$

Using these results, we have the following corollary.

Corollary 6.3. *For a set A in $\mathbb{C}$, let $T(A)$ be the number of collinear triples of points in $A \times A$. Then we have*

$$T(A) \lesssim |A|^4.$$

Proof. Let L_k be the set of lines l such that $2^k \leq |l \cap (A \times A)| < 2^{k+1}$. Since $|l \cap (A \times A)| \leq |A|$ for any l, we have $k \leq \log_2 |A|$. Thus, using Corollary 6.2, we have

$$\begin{aligned} T(A) &\leq \sum_{k=0}^{\log_2 |A|} \sum_{l \in L_k} |l \cap (A \times A)|^3 \\ &\leq \sum_{k=0}^{\log_2 |A|} \left(\frac{|A|^4}{2^{3k}} + \frac{|A|^2}{2^k}\right) \cdot 2^{3k+3} \\ &\leq \sum_{k=0}^{\log_2 |A|} 8|A|^4 + \sum_{k=0}^{\log_2 |A|} 8|A|^2 2^{2k} \lesssim |A|^4, \end{aligned}$$

where we have used the fact that $2^k \leq |A|$. □

Lemma 6.4. *Let A be a set in $\mathbb{C}$ with $|A| \geq 2$. Denote by $\Lambda^\times(A)$ the number of quadruples $(a, b, c, d) \in A^4$ such that $ab = cd$. Then the number of tuples $(a, b, c, a', b', c') \in A^6$ such that*

$$a(b - c) = a'(b' - c')$$

is $\lesssim \Lambda^\times(A)^{1/2}|A|^3 + |A|^4 \leq 2\Lambda^\times(A)^{1/2}|A|^3$.

Proof. Since $|A| \geq 2$, without loss of generality, we assume that $0 \notin A$. We first have an observation that the number of desired tuples with $b = c$ or $b' = c'$ is at most $|A|^4 \leq \Lambda^\times(A)^{1/2}|A|^3$ since $\Lambda^\times(A) \geq |A|^2$.

Let M be the number of tuples with $b \neq c$ and $b' \neq c'$. We have M is equal to the number of desired tuples $(a, b, c, a', b', c') \in A^6$ such that

$$\frac{a}{a'} = \frac{b' - c'}{b - c}.$$

Using the Cauchy–Schwarz inequality, we have

$$M \leq \Lambda^\times(A)^{1/2} \cdot \left|\left\{(b_1, c_1, b_2, c_2, b_3, c_3, b_4, c_4) \in A^8 : \frac{b_1 - c_1}{b_2 - c_2} = \frac{b_3 - c_3}{b_4 - c_4}\right\}\right|^{1/2}.$$

Using the Cauchy–Schwarz inequality one more time, we have

$$\begin{aligned}
&\left|\left\{(b_1, c_1, b_2, c_2, b_3, c_3, b_4, c_4) \in A^8 : \frac{b_1 - c_1}{b_2 - c_2} = \frac{b_3 - c_3}{b_4 - c_4}\right\}\right| \\
&\qquad \le |A|^2 \cdot \left|\left\{(b_1, c_1, b_2, c_2, d_1, d_2) \in A^6 : \frac{b_1 - c_1}{b_2 - c_2} = \frac{d_1 - c_1}{d_2 - c_2}\right\}\right| \\
&\qquad \le |A|^2 \cdot T(A) \lesssim |A|^6,
\end{aligned}$$

where we have used Corollary 6.3 in the last inequality. Hence, $M \lesssim \Lambda^\times(A)^{1/2}|A|^3$. This completes the proof of theorem. □

Proof of Theorem 1.9. Without loss of generality, we assume that $0 \notin A$. It has been proved in [Rudnev et al. 2020] that there exist $B, C \subset A$ such that $|B|, |C| \ge |A|/3$ and

$$\Lambda^+(B) \cdot \Lambda^\times(C) \lesssim |A|^{11/2}.$$

This implies that $\Lambda^+(B) \lesssim |A|^{11/4}$ or $\Lambda^\times(C) \lesssim |A|^{11/4}$. If $\Lambda^+(B) \lesssim |A|^{11/4}$ then we replace the set A in the Theorem 1.9 by B, otherwise, we replace the set A by C. Thus, we may assume that either $\Lambda^+(A) \lesssim |A|^{11/4}$ or $\Lambda^\times(A) \lesssim |A|^{11/4}$

The rest of proof of Theorem 1.9 is almost identical with that of Theorem 1.8, and the last step is to estimate X.

Using Theorem 6.1 and the same argument as in the proof of Theorem 1.8, we have

$$X \lesssim |A|^3 \Lambda^+(A)^{1/2}.$$

On the other hand, using Lemma 6.4, we have

$$X \lesssim |A|^3 \Lambda^\times(A)^{1/2}.$$

Since either $\Lambda^+(A) \lesssim |A|^{11/4}$ or $\Lambda^\times(A) \lesssim |A|^{11/4}$, we have

$$X \lesssim |A|^{3+11/8}.$$

Therefore, $|[A, A, 0][A, A, 0]| \gtrsim |A|^{5-11/8} = |A|^{29/8} = |[A, A, 0]|^{29/16}$. This completes the proof of the theorem. □

Acknowledgments

The authors would like to thank the referee for useful comments and suggestions.

Doowon Koh was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MIST) (NRF-2018R1D1A1B07044469). Thang Pham was supported by Swiss National Science Foundation grant P400P2-183916.

Le Quang Ham and Le Anh Vinh were supported by the National Foundation for Science and Technology Development Project, No. 101.99-2019.318.

References

[Elekes and Tóth 2005] G. Elekes and C. D. Tóth, "Incidences of not-too-degenerate hyperplanes", pp. 16–21 in *Computational geometry* (*SCG'05*) (Pisa, 2005), ACM, New York, 2005. MR Zbl

[Hegyvári and Hennecart 2012] N. Hegyvári and F. Hennecart, "A note on Freiman models in Heisenberg groups", *Israel J. Math.* **189** (2012), 397–411. MR Zbl

[Hegyvári and Hennecart 2013] N. Hegyvári and F. Hennecart, "A structure result for bricks in Heisenberg groups", *J. Number Theory* **133**:9 (2013), 2999–3006. MR Zbl

[Hegyvári and Hennecart 2018] N. Hegyvári and F. Hennecart, "Expansion for cubes in the Heisenberg group", *Forum Math.* **30**:1 (2018), 227–236. MR Zbl

[Koh et al. 2018] D. Koh, T. Pham, and L. A. Vinh, "Extension theorems and distance problems over finite fields", preprint, 2018. arXiv

[Lund and Petridis 2018] B. Lund and G. Petridis, "Bisectors and pinned distances", preprint, 2018. arXiv

[Macourt et al. 2018] S. Macourt, I. D. Shkredov, and I. E. Shparlinski, "Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields", *Canad. J. Math.* **70**:6 (2018), 1319–1338. MR Zbl

[Murphy et al. 2017] B. Murphy, M. Rudnev, I. D. Shkredov, and Y. N. Shteinikov, "On the few products, many sums problem", preprint, 2017. arXiv

[Rudnev and Shkredov 2018] M. Rudnev and I. D. Shkredov, "On growth rate in $\mathrm{SL}_2(\mathbb{F}_p)$, the affine group and sum-product type implications", preprint, 2018. arXiv

[Rudnev et al. 2020] M. Rudnev, I. Shkredov, and S. Stevens, "On the energy variant of the sum-product conjecture", *Rev. Mat. Iberoam.* **36**:1 (2020), 207–232. MR

[Shkredov 2020] I. D. Shkredov, "Some remarks on products of sets in the Heisenberg group and in the affine group", *Forum Math.* **32**:1 (2020), 189–199. MR

[Stevens and de Zeeuw 2017] S. Stevens and F. de Zeeuw, "An improved point-line incidence bound over arbitrary fields", *Bull. Lond. Math. Soc.* **49**:5 (2017), 842–858. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2006. MR Zbl

[Tóth 2015] C. D. Tóth, "The Szemerédi–Trotter theorem in the complex plane", *Combinatorica* **35**:1 (2015), 95–126. MR Zbl

Received August 10, 2019. Revised November 21, 2019.

DAO NGUYEN VAN ANH
THE OLYMPIA SCHOOLS HANOI
HANOI
VIETNAM
anh.dnv@theolympiaschools.edu.vn

LE QUANG HAM
UNIVERSITY OF SCIENCE
VIETNAM NATIONAL UNIVERSITY HANOI
HANOI
VIETNAM
hamlaoshi@gmail.com

DOOWON KOH
DEPARTMENT OF MATHEMATICS
CHUNGBUK NATIONAL UNIVERSITY
CHEONGJU CITY
SOUTH KOREA
koh131@chungbuk.ac.kr

THANG PHAM
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ROCHESTER
ROCHESTER, NY
UNITED STATES
vanthangpham@rochester.edu

LE ANH VINH
UNIVERSITY OF EDUCATION
VIETNAM NATIONAL UNIVERSITY - HANOI
VIETNAM INSTITUTE OF EDUCATIONAL SCIENCES
HANOI
VIETNAM
vinhla@vnu.edu.vn

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
matthias@math.ucla.edu

Paul Balmer
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
balmer@math.ucla.edu

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Daryl Cooper
Department of Mathematics
University of California
Santa Barbara, CA 93106-3080
cooper@math.ucsb.edu

Wee Teck Gan
Mathematics Department
National University of Singapore
Singapore 119076
matgwt@nus.edu.sg

Kefeng Liu
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
liu@math.ucla.edu

Jiang-Hua Lu
Department of Mathematics
The University of Hong Kong
Pokfulam Rd., Hong Kong
jhlu@maths.hku.hk

Sorin Popa
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
popa@math.ucla.edu

Jie Qing
Department of Mathematics
University of California
Santa Cruz, CA 95064
qing@cats.ucsc.edu

Paul Yang
Department of Mathematics
Princeton University
Princeton NJ 08544-1000
yang@math.princeton.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

SUPPORTING INSTITUTIONS

ACADEMIA SINICA, TAIPEI
CALIFORNIA INST. OF TECHNOLOGY
INST. DE MATEMÁTICA PURA E APLICADA
KEIO UNIVERSITY
MATH. SCIENCES RESEARCH INSTITUTE
NEW MEXICO STATE UNIV.
OREGON STATE UNIV.
STANFORD UNIVERSITY
UNIV. OF BRITISH COLUMBIA
UNIV. OF CALIFORNIA, BERKELEY
UNIV. OF CALIFORNIA, DAVIS
UNIV. OF CALIFORNIA, LOS ANGELES
UNIV. OF CALIFORNIA, RIVERSIDE
UNIV. OF CALIFORNIA, SAN DIEGO
UNIV. OF CALIF., SANTA BARBARA
UNIV. OF CALIF., SANTA CRUZ
UNIV. OF MONTANA
UNIV. OF OREGON
UNIV. OF SOUTHERN CALIFORNIA
UNIV. OF UTAH
UNIV. OF WASHINGTON
WASHINGTON STATE UNIVERSITY

These supporting institutions contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its contents or policies.

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2020 is US $520/year for the electronic version, and $705/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2020 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 305 No. 2 April 2020

0030-8730(2020)305:2;1-Q